



# Monitoreo de aplicaciones y la infraestructura



# INTRODUCCIÓN

La capacidad de monitorear sus aplicaciones e infraestructura es fundamental para brindar servicios de TI confiables y consistentes. Los requisitos de monitoreo varían desde la recopilación de estadísticas para análisis a largo plazo hasta la reacción rápida a cambios e interrupciones. El monitoreo también puede respaldar la generación de informes de cumplimiento al verificar continuamente que la infraestructura cumpla con los estándares organizacionales.

## OBJETIVOS

- Crear y Utilice el comando de ejecución de AWS Systems Manager para instalar el agente CloudWatch en instancias de Amazon EC2.
- Supervisar los registros de aplicaciones mediante el agente CloudWatch y CloudWatch Logs.
- Supervise las métricas del sistema mediante el agente CloudWatch y CloudWatch Metrics
- Cree notificaciones en tiempo real utilizando CloudWatch Events
- Seguimiento del cumplimiento de la infraestructura mediante AWS Config.



# TAREA 1

En esta tarea, se utiliza Systems Manager para instalar el agente de CloudWatch en una instancia de EC2. Se configura para recopilar métricas de la aplicación y del sistema.

- En la consola de administración de AWS, en ServiciosMenú, seleccione Administrador de sistemas.
- En el panel de navegación izquierdo, seleccione Ejecutar comando.
- Seleccione Ejecutar un comando
- Seleccione el botón junto a `AWS-ConfigureAWSPackage` (normalmente aparece en la parte superior de la lista).

**Documento de comando**  
Seleccione el tipo de comando que desea ejecutar.

< 1 2 3 4 ... >

	Nombre	Propietario	Tipos de plataformas
<input type="radio"/>	<a href="#">AWS-ApplyAnsiblePlaybooks</a>	Amazon	Linux
<input type="radio"/>	<a href="#">AWS-ApplyChefRecipes</a>	Amazon	Windows, Linux
<input type="radio"/>	<a href="#">AWS-ApplyDSCMofs</a>	Amazon	Windows
<input type="radio"/>	<a href="#">AWS-ApplyPatchBaseline</a>	Amazon	Windows
<input checked="" type="radio"/>	<a href="#">AWS-ConfigureAWSPackage</a>	Amazon	Windows, Linux, MacOS
<input type="radio"/>	<a href="#">AWS-ConfigureCloudWatch</a>	Amazon	Windows
<input type="radio"/>	<a href="#">AWS-ConfigureDocker</a>	Amazon	Windows, Linux
<input type="radio"/>	<a href="#">AWS-ConfigureKernelLivePatching</a>	Amazon	Linux
<input type="radio"/>	<a href="#">AWS-ConfigureWindowsUpdate</a>	Amazon	Windows
<input type="radio"/>	<a href="#">AWS-FindWindowsUpdates</a>	Amazon	Windows



- Desplácese hasta la sección Parámetros de comando y configure la siguiente información:

**Parámetros de comando**

**Action**  
(Required) Specify whether to install or uninstall the package.

**Installation Type**  
(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.

**Installation Type**  
(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.

**Name**  
(Required) The package to install/uninstall.

**Version**  
(Optional) The version of the package to install or uninstall. If you don't specify a version, the system installs the latest published version by default. The system will only attempt to uninstall the version that is currently installed. If no version of the package is installed, the system returns an error.

**Additional Arguments**  
(Optional) The additional parameters to provide to your install, uninstall, or update scripts.

- En la sección Objetivos, Seleccione instancias manualmente y luego, en Instancias, seleccione la casilla de verificación junto a Servidor web.

**Destinos**

**Destinos**  
Elija un método para seleccionar los destinos.

☐ Especificar etiquetas de instancia  
Especifique uno o más pares clave-valor de etiqueta para seleccionar las instancias que comparten esas etiquetas.

☒ Elegir instancias de forma manual  
Seleccione manualmente las instancias que desea registrar como destinos.

☐ Elegir un grupo de recursos  
Elija un grupo de recursos que incluya los recursos que desea enviar a los destinos.

**Instancias**




< 1 >

<input checked="" type="checkbox"/>	Nombre	ID de la instancia	Estado de la instancia	Zona de disponibilidad	Estado del ping
<input checked="" type="checkbox"/>	Web Server	i-08caa9fe6947ffdc6	running	us-west-2a	Online

- En la parte inferior de la página, seleccione Ejecutar
- Espere a que el estado general cambie a Éxito. Ocasionalmente, puede elegir el botón Actualice hacia la parte superior de la página para actualizar el estado.



- En Objetivos y resultados, seleccione el botón junto a la instancia y luego haga clic en Ver salida.

Destinos y salidas					Ver salida
<input type="text" value="Search command invocations"/>					< 1 >
ID de instancia	Nombre de instancia	Estado	Estado detallado	Hora de inicio	
 i-08caa9fe6947ffdc6	ip-10-0-0-27.us-west-2.compute.internal	 Correcto	 Correcto	Fri, 04 Oct 2024 2	

- Expandir Paso 2 – Salida.

**▼ Output**

The command output displays a maximum of 24,000 characters. You can view the complete command output in either Amazon S3 or CloudWatch Logs, if you specify an S3 bucket or a logs group when you run the command.


```
Initiating arn:aws:ssm:::package/AmazonCloudWatchAgent
1.300044.0b793 install


Plugin aws:runShellScript ResultStatus Success

install output: Running sh install.sh

create group cwagent, result: 0

create user cwagent, result: 0
```

 Copy

 Download

- En el panel de navegación izquierdo, seleccione Almacén de parámetros.
- Seleccione Crear parámetro y luego configure la siguiente información:

**Detalles del parámetro**

**Nombre**

Al asignar un nombre a un parámetro, puede utilizar barras diagonales (/) para organizarlo en una jerarquía. [Más información sobre las jerarquías](#)

**Descripción — Optional**

- Seleccione Crear parámetro.
- En el panel de navegación izquierdo, seleccione Ejecutar comando.
- Seleccione el comando Ejecutar
- Elige elcuadro y luego seleccione lo siguiente:



**Documento de comando**  
Seleccione el tipo de comando que desea ejecutar.

Buscar por palabra clave o filtrar por etiqueta o atributos

Prefijo del nombre del documento: Equals: AmazonCloudWatch-ManagedAgent X Clear filters < 1 >

	Nombre	Propietario	Tipos de plataformas
<input type="radio"/>	<a href="#">AmazonCloudWatch-ManagedAgent</a>	Amazon	Windows, Linux, MacOS

- o Elija AmazonCloudWatch-ManagedAgent (elija el nombre en sí).
- o Seleccione la pestaña Contenido y desplácese hasta la parte inferior para ver el script real que se ejecutará en la instancia de destino.

AWS Systems Manager > Documentos > AmazonCloudWatch-ManagedAgent

### AmazonCloudWatch-ManagedAgent

Eliminar Acciones Ejecutar comando

Descripción **Contenido** Versiones Detalles

Versión del documento  
8 (Predeterminada)

El contenido de este documento es el siguiente:

```
1 - {
2   "schemaVersion": "2.2",
3   "description": "Send commands to Amazon Cloudwatch Agent",
4   "parameters": {
5     "action": {
6       "description": "The action Cloudwatch Agent should take.",
7       "type": "String",
8       "default": "configure",
9       "allowedValues": [
10        "configure",
11        "configure (append)",
12        "configure (remove)",
13        "start",
14        "status",
15        "stop"
16      ]
17    },
18    "mode": {
19      "description": "Controls platform-specific default behavior such as whether to include EC2 Metadata in metrics.",
20      "type": "String",
21      "default": "ec2",
22      "allowedValues": [
23        "ec2",
24        "onPremise",
25        "auto"
26      ]
27    },
28    "optionalConfigurationSource": {
29      "description": "Only for 'configure' related actions. Use 'ssm' to apply a ssm parameter as config. Use 'default' to apply default config for amazon-cloudwatch-agent. Use 'all' to apply all default config.",
30      "type": "String",
31      "allowedValues": [
32        "ssm",
33        "default",
34        "all"
35      ],
36      "default": "ssm"
37    },
38    "optionalConfigurationLocation": {
39      "description": "Only for 'configure' related actions. Only needed when Optional Configuration Source is set to 'ssm'. The value should be a ssm parameter name.",
40      "type": "String"
41    }
42  }
43 }
```

- o Cierre la pestaña actual del navegador web, lo que debería regresarlo a la pestaña Ejecutar un comando que estaba usando anteriormente.
- o En la sección Parámetros de comando, configure la siguiente información:



### Parámetros de comando

**Action**  
The action CloudWatch Agent should take.

configure ▼

**Mode**  
Controls platform-specific default behavior such as whether to include EC2 Metadata in metrics.

ec2 ▼

**Optional Configuration Source**  
Only for 'configure' related actions. Use 'ssm' to apply a ssm parameter as config. Use 'default' to apply default config for amazon-cloudwatch-agent. Use 'all' with 'configure (remove)' to clean all configs for amazon-cloudwatch-agent.

ssm ▼

**Optional Configuration Location**  
Only for 'configure' related actions. Only needed when Optional Configuration Source is set to 'ssm'. The value should be a ssm parameter name.

Monitor-Web-Server

**Optional Restart**  
Only for 'configure' related actions. If 'yes', restarts the agent to use the new configuration. Otherwise the new config will only apply on the next agent restart.

yes ▼

- En la sección Objetivos, Seleccione instancias manualmente.
- En la sección Instancias, seleccione la casilla de verificación junto a Servidor web.

### Destinos

**Destinos**  
Elija un método para seleccionar los destinos.

☐ Especificar etiquetas de instancia  
Especifique uno o más pares clave-valor de etiqueta para seleccionar las instancias que comparten esas etiquetas.

☒ Elegir instancias de forma manual  
Seleccione manualmente las instancias que desea registrar como destinos.

☐ Elegir un grupo de recursos  
Elija un grupo de recursos que incluya los recursos que desea enviar a los destinos.

i-08caa9fe6947ffdc6 X

### Instancias

Q

< 1 >

<input checked="" type="checkbox"/>	Nombre	ID de la instancia	Estado de la instancia	Zona de disponibilidad	Estado del ping
<input checked="" type="checkbox"/>	Web Server	i-08caa9fe6947ffdc6	running	us-west-2a	Online

- Seleccione Ejecutar.
- Espere a que el estado general cambie a Éxito.

### Estado del comando

Estado general  
✔ Correcto

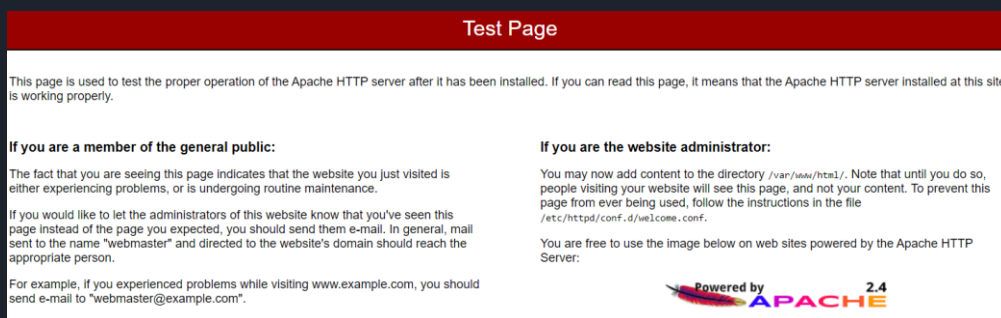
Estado detallado  
✔ Correcto



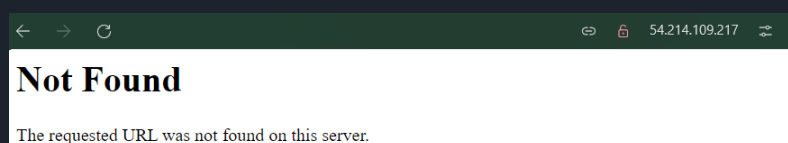
## TAREA 2

En esta tarea, generará datos de registro en el servidor web y luego supervisará los registros mediante CloudWatch Logs.

- Seleccione el menú desplegable Detalles encima de estas instrucciones y luego seleccione Mostrar.
- Abra una nueva pestaña del navegador web, pegue el WebServerIP que copió y luego presione Entrar.



- Agreguelo /starta la URL del navegador y presione Enter.




- Mantenga esta pestaña abierta en su navegador web, pero regrese a la pestaña del navegador que muestra la Consola de administración de AWS.
- De los ServiciosEn el menú, seleccione CloudWatch.
- En el panel de navegación izquierdo, seleccione Grupos de registros.






### Grupos de registros (2)

 Acciones ▼ Ver en Logs Insights Empezar a seguir [Crear un grupo de registros](#)


De forma predeterminada, solo cargamos hasta 10 000 grupos de registros.

☐ Coincidencia exacta < 1 > 

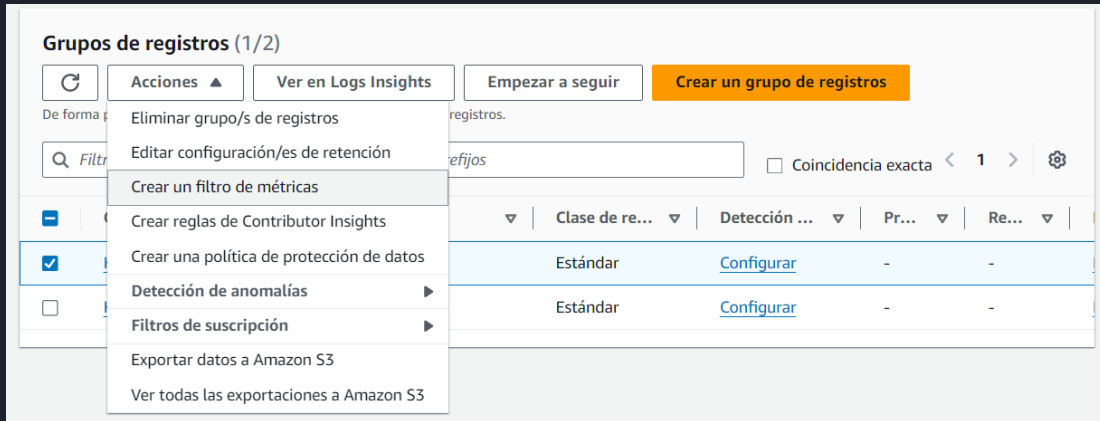
<input type="checkbox"/>	Grupo de registros	Clase de re...	Detección ...	Pr...	Re...	R
<input type="checkbox"/>	<a href="#">HttpAccessLog</a>	Estándar	<a href="#">Configurar</a>	-	-	N
<input type="checkbox"/>	<a href="#">HttpErrorLog</a>	Estándar	<a href="#">Configurar</a>	-	-	N

- Seleccione HttpAccessLog (elija el nombre en sí).
- En la sección Flujos de registros, seleccione el flujo de registros en la tabla (elija el nombre). Tiene el mismo ID que la instancia EC2 a la que está asociado el registro.

▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:10 +0000]	"GET /admin/vendor/phpunit/phpunit/src/Util/PHP/...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:11 +0000]	"GET /backup/vendor/phpunit/phpunit/src/Util/PHP/...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:11 +0000]	"GET /blog/vendor/phpunit/phpunit/src/Util/PHP/e...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:11 +0000]	"GET /workspace/drupal/vendor/phpunit/phpunit/sr...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:11 +0000]	"GET /panel/vendor/phpunit/phpunit/src/Util/PHP/...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:12 +0000]	"GET /public/vendor/phpunit/phpunit/src/Util/PHP/...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:12 +0000]	"GET /apps/vendor/phpunit/phpunit/src/Util/PHP/e...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:12 +0000]	"GET /app/vendor/phpunit/phpunit/src/Util/PHP/ev...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:12 +0000]	"GET /index.php?s=/index/\\think\\app\\invokefunc...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:12 +0000]	"GET /public/index.php?s=/index/\\think\\app\\inv...
▶	2024-10-04T20:49:19.193Z	27.210.154.97	- - [04/Oct/2024:20:25:13 +0000]	"GET /index.php?lang=../../../../../usr...
▶	2024-10-04T20:49:24.544Z	27.210.154.97	- - [04/Oct/2024:20:25:13 +0000]	"GET /index.php?lang=../../../../../tmp...
▶	2024-10-04T21:11:54.193Z	185.224.128.59	- - [04/Oct/2024:21:11:50 +0000]	"GET /cgi-bin/luci/stok=/locale HTTP/1.1" 404 ...
▶	2024-10-04T21:28:43.193Z	147.185.132.18	- - [04/Oct/2024:21:28:38 +0000]	"GET / HTTP/1.1" 403 3630 "-" "Expansive, a Palo ...
▶	2024-10-04T21:31:43.193Z	45.156.130.4	- - [04/Oct/2024:21:31:38 +0000]	"GET / HTTP/1.1" 403 3630 "-" "Mozilla/5.0 (Windo...
▶	2024-10-04T21:37:32.717Z	190.234.179.20	- - [04/Oct/2024:21:37:32 +0000]	"GET / HTTP/1.1" 403 3630 "-" "Mozilla/5.0 (Win...
▶	2024-10-04T21:37:32.967Z	190.234.179.20	- - [04/Oct/2024:21:37:32 +0000]	"GET /icons/apache_pb2.gif HTTP/1.1" 200 4234 "...
▶	2024-10-04T21:37:37.193Z	190.234.179.20	- - [04/Oct/2024:21:37:32 +0000]	"GET /favicon.ico HTTP/1.1" 404 196 "http://54...
▼	2024-10-04T21:39:00.192Z	190.234.179.20	- - [04/Oct/2024:21:38:56 +0000]	"GET /start HTTP/1.1" 404 196 "-" "Mozilla/5.0 ...
		190.234.179.20	- - [04/Oct/2024:21:38:56 +0000]	"GET /start HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36"

No hay eventos recientes en este momento. [Reintentar](#) [Volver arriba](#) 

- En el panel de navegación izquierdo, seleccione Grupos de registros.
- Seleccione la casilla de verificación junto a HttpAccessLog.
- En el menú desplegable Acciones, seleccione Crear filtro de métricas.



- ## Crear patrón de filtro
- Puede usar filtros de métricas para monitorear los eventos de un grupo de registros cuando se envíen a CloudWatch Logs. Puede monitorear y contar términos específicos o extraer valores de los eventos de registro, así como asociar los resultados a una métrica. [Más información acerca de la sintaxis de los patrones.](#) 
- ### Patrón del filtro
- Especifique los términos o el patrón que deben tener los eventos de registro para crear métricas.
- 

- ## Probar patrón

Seleccionar los datos de registro para probar

Mensajes de eventos de registro

Escriba los datos de registro para probarlos con el patrón de filtro. Utilice saltos de línea para separar los eventos de registro.

```
27.210.154.97 -- [04/Oct/2024:20:25:03 +0000] "POST /cgi-bin/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/bin/sh HTTP/1.1" 400 226 "-" "Custom-AsyncHttpClient"
27.210.154.97 -- [04/Oct/2024:20:25:03 +0000] "POST /hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input HTTP/1.1" 404 196
```

Probar patrón

Resultados

Seleccione los mensajes de eventos de registro anteriores y haga clic en Probar patrón para ver los resultados.



- Elija el patrón de prueba
- En la sección Resultados, seleccione Mostrar resultados de la prueba.

▼ Mostrar resultados de la prueba

	\$status_code	\$timestamp	\$user
	404	04/Oct/2024:20:25:03 +0000	-
	404	04/Oct/2024:20:25:03 +0000	-
	404	04/Oct/2024:20:25:04 +0000	-
	404	04/Oct/2024:20:25:04 +0000	-
	404	04/Oct/2024:20:25:04 +0000	-
	404	04/Oct/2024:20:25:04 +0000	-

- Elija Siguiente.
- En la sección Crear nombre de filtro, en el cuadro Nombre del filtro, ingrese 404Errors

**Crear nombre de filtro**

Los eventos de registro que coincidan con el patrón que defina se registrarán en la métrica que especifique. Puede diagramar la métrica y establecer alarmas para recibir notificaciones.

Nombre del filtro

Patrón del filtro

- En la sección Detalles de métricas, configure la siguiente información:

**Detalles de la métrica**

**Espacio de nombres de métrica**  
Namespaces let you group similar metrics. [Más información](#)

☒ Crear nuevo  
Los espacios de nombres pueden tener una longitud máxima de 255 caracteres; todos los caracteres son válidos excepto los dos puntos (:) al comienzo del nombre.

**Nombre de métrica**  
El nombre de métrica identifica esta métrica y debe ser único dentro del espacio de nombres. [Más información](#)

El nombre de la métrica puede tener un máximo de 255 caracteres; todos los caracteres son válidos, excepto los dos puntos (:), el asterisco (\*), el dólar (\$) y el espacio ( ).

**Valor de métrica**  
El valor de métrica es el valor publicado en el nombre de métrica cuando hay coincidencias con el patrón de filtro.



- Seleccione Siguiente. Si la opción Siguiente no está habilitada, haga clic en un campo de texto vacío; esto cambiará el foco y la habilitará.
- En la página Revisar y crear, seleccione Crear filtro de métricas.

Se ha creado el filtro de métricas "404Errors".

CloudWatch > Grupos de registros > HttpAccessLog

### HttpAccessLog

Acciones ▼ Ver en Logs Insights Empezar a seguir Buscar el grupo de registros

▼ Detalles del grupo de registros

Clase de registro	Información	Bytes almacenados	ID de clave de KMS
Estándar		-	-
ARN	Filtros de métricas	Detección de anomalías	
arn:aws:logs:us-west-2:107791249488:log-group:HttpAccessLog:*	1	Configurar	
Hora de creación	Filtros de suscripción	Protección de datos	
Hace 1 hora	0	-	
Retención	Reglas de Contributor Insights	Recuento de datos confidenciales	
No vence nunca	-	-	

- En el panel Errores 404, seleccione la casilla de verificación en la esquina superior derecha.
- En la sección Filtros de métricas, elija Crear alarma

Filtros de métricas (1/1) Editar Eliminar Crear alarma 1/2 Crear un filtro de métricas

Find metric filters

404Errors ☒

Patrón del filtro  
[ip, id, user, timestamp, request, status\_code=404, size]

Métrica  
LogMetrics 1/2 / 404Errors 1/2

Valor de métrica  
1

Valor predeterminado  
-

Unit  
-

Dimensiones  
-

Alarms  
None.



- Configure los siguientes ajustes:

4 ————— 20:00 21:00 22:00

■ 404Errors

Período  
1 minuto ▼

### Condiciones

Tipo de límite

☒ Estático  
Utilice un valor como límite

☐ Detección de anomalías  
Utilice una banda como límite

Cuando 404Errors sea...  
Defina la condición de la alarma.

☐ Mayor  
> límite

☒ Mayor/Igual  
≥ límite

☐ Menor/Igual  
≤ límite

☐ Menor  
< límite

que...  
Defina el valor del límite.

5

Debe ser un número

- En la sección Notificación, configure lo siguiente:

Enviar una notificación al siguiente tema de SNS  
Defina el tema de SNS (Simple Notification Service) que recibirá la notificación.

☐ Seleccione un tema de SNS existente

☒ Crear un tema nuevo

☐ Usar ARN del tema para notificar a otras cuentas

Crear un nuevo tema...  
El nombre del tema debe ser único.

Default\_CloudWatch\_Alarms\_Topic

Los nombres de los temas de SNS solo pueden contener caracteres alfanuméricos, guiones (-) y guiones bajos (\_).

Puntos de enlace de correo electrónico que recibirán la notificación...  
Añada una lista de direcciones de correo electrónico separadas por comas. Cada dirección se agregará como una suscripción al tema anterior.

josephh2408@gmail.com

usuario1@ejemplo.com, usuario2@ejemplo.com

Crear un tema

- Para Nombre y descripción, configure los siguientes ajustes:

### Nombre y descripción

Nombre de la alarma

404 Errors

Descripción de la alarma - *opcional* [Ver las pautas de formato](#)

[Editar](#) | [Vista previa](#)

Alert when too many 404s detected on an instance


Hasta 1024 caracteres (48/1024)


**El formato Markdown solo se aplica al ver la alarma en la consola. La descripción permanecerá en texto plano en las notificaciones de alarma.**



- Seleccione Crear alarma
- Vaya a su correo electrónico, busque un mensaje de confirmación y seleccione el enlace Confirmar suscripción.
- Regrese a la consola de administración de AWS.
- En el panel de navegación izquierdo, seleccione CloudWatch (en la parte superior).
- Regrese a la pestaña del navegador web con el servidor web.
- Intente acceder a páginas que no existen agregando un nombre de página después de la dirección IP. Repita este paso al menos cinco veces.
- Espere entre 1 y 2 minutos para que se active la alarma. En la consola de administración de AWS, puede elegir ocasionalmente Actualizar para actualizar el estado.
- Revisa tu correo electrónico. Deberías haber recibido un correo electrónico con el asunto ALARMA: "Errores 404".

**ALARMA: "404 Errors" in US West (Oregon)** Recibidos x

 **AWS Notifications** <no-reply@sns.amazonaws.com>  
para mí ▼ 17:22 (hace 0 minutos) ☆ 😊 ↶ ⋮

 Traducir al español X

You are receiving this email because your Amazon CloudWatch Alarm "404 Errors" in the US West (Oregon) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [8.0 (04/10/24 22:21:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Friday 04 October, 2024 22:22:20 UTC".

View this alarm in the AWS Management Console:  
<https://us-west-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-west-2#alarmsV2:alarm/404%20Errors>

Alarm Details:

- Name: 404 Errors
- Description: Alert when too many 404s detected on an instance
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [8.0 (04/10/24 22:21:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Friday 04 October, 2024 22:22:20 UTC
- AWS Account: 107791249488
- Alarm Arn: arn:aws:cloudwatch:us-west-2:107791249488:alarm:404 Errors

Threshold:

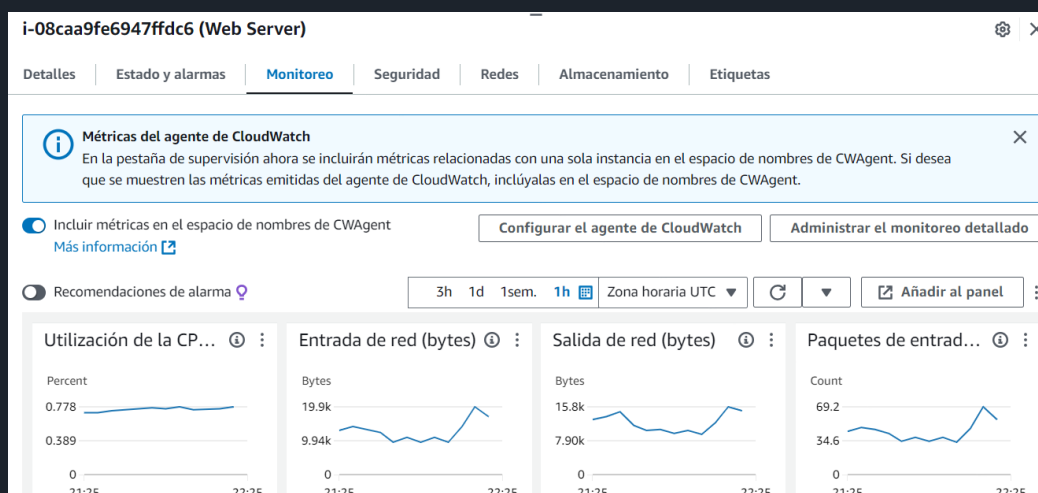
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 5.0 for at least 1 of the last 1 period(s) of 60 seconds.



# TAREA 3

Las métricas son datos sobre el rendimiento de sus sistemas. CloudWatch almacena métricas de los servicios de AWS que utiliza. También puede publicar sus propias métricas de aplicaciones a través del agente de CloudWatch o directamente desde su aplicación. CloudWatch puede presentar las métricas para búsquedas, gráficos, paneles y alarmas. En la tarea, utiliza métricas que proporciona CloudWatch.

- Sobre los Servicios En el menú, seleccione EC2.
- En el panel de navegación izquierdo, seleccione Instancias.
- Seleccione la casilla de verificación junto a Servidor web.
- Seleccione la pestaña Monitoreo en la mitad inferior de la página.





- Desde el menú Servicios, seleccione CloudWatch.
- En el panel de navegación izquierdo, seleccione Métricas. Luego, expanda Métricas y seleccione Todas las métricas.
- Seleccione CWAgent y luego elija dispositivo, fstype, host, ruta.
- Sobre la tabla, elija CWAgent (en la línea que dice Todo > CWAgent > dispositivo, fstype, host, ruta).

The screenshot shows the AWS CloudWatch Metrics console. The top navigation bar includes 'Examinar', 'Consulta de múltiples orígenes', 'Métricas diagramadas', 'Opciones', and 'Origen'. The main section is titled 'Métricas (12) Información'. Below the title, there are buttons for 'Recomendaciones de alarma', 'Descargar código de alarma', 'Crear alarma', 'Gráfico con SQL', and 'Búsqueda en gráficos'. A breadcrumb trail shows 'Oregon > Todo > CWAgent > device, fstype, host, path'. A search bar contains the text 'Buscar cualquier métrica, dimensión, ID de recurso o ID de cuenta'. Below the search bar, a table lists metrics:

<input type="checkbox"/>	device 12/12	fstype	host	path	Nombre de métrica
<input type="checkbox"/>	devtmpfs	devt...	ip-10-0-0-27.us-west-2.compute.internal	/dev	disk_used_percent ⓘ
<input type="checkbox"/>	devtmpfs	devt...	ip-10-0-0-27.us-west-2.compute.internal	/dev	disk_inodes_free ⓘ
<input type="checkbox"/>	nvme0n1p1	xfs	ip-10-0-0-27.us-west-2.compute.internal	/	disk_inodes_free ⓘ

- Seleccione el host.
- Sobre la tabla, seleccione Todos (en la línea que dice Todos > CWAgent > dispositivo, fstype, host, ruta).

The screenshot shows the AWS CloudWatch Metrics console with the view filtered to a specific host. The breadcrumb trail is 'Oregon > Todo > CWAgent > host'. The table lists metrics for the host:

<input type="checkbox"/>	host 2/2	Nombre de métrica	Alarmas
<input type="checkbox"/>	ip-10-0-0-27.us-west-2.compute.internal	swap_used_percent ⓘ	Sin alarmas
<input type="checkbox"/>	ip-10-0-0-27.us-west-2.compute.internal	mem_used_percent ⓘ	Sin alarmas

- Sobre Sobre la tabla, seleccione Todos (en la línea que dice Todos > CWAgent > dispositivo, fstype, host, ruta ).
- Explore las otras métricas que captura CloudWatch. Se trata de métricas generadas automáticamente que provienen de





los servicios de AWS que se han utilizado en esta cuenta de AWS.

Agregar matemática ▼

Agregar consulta ▼

Examinar

Consulta de múltiples orígenes

Métricas diagramadas

Opciones

Origen

▼ Espacios de nombres personalizados

CWAgent17

LogMetrics1

▼ Espacios de nombres de AWS

EBS10

• Ver el panel automático

EC220

• Ver el panel automático

Eventos8

• Ver el panel automático

Registros19

• Ver el panel automático

SNS4

SSM Run Command3



# TAREA 4

En esta tarea, creará una notificación en tiempo real que le informará cuando se detiene o finaliza una instancia.

- o En el panel de navegación izquierdo, expanda Eventos, seleccione Reglas.
- o Seleccione Crear regla.
- o En la sección Origen del evento, configure los siguientes ajustes:

**Patrón de eventos** Información

**Origen del evento**  
Servicio de AWS o socio de EventBridge como origen

Servicios de AWS ▼

**Servicio de AWS**  
Nombre del servicio de AWS como origen del evento

EC2 ▼

**Tipo de evento**  
El tipo de evento como origen del patrón coincidente

EC2 Instance State-change Notification ▼

**Especificación del tipo de evento 1**  
El tipo de evento como origen del patrón coincidente

☐ Cualquier estado

☒ Estados específicos

**Estados específicos**

stopping × terminated ×

**Especificación del tipo de evento 2**

☒ Cualquier instancia

☐ Identificadores de instancia específicos

**Patrón de eventos**  
Patrón de eventos o filtro para que coincidan con los eventos

```
1 {  
2   "source": ["aws.ec2"],  
3   "detail-type": ["EC2 Instance State-change Notification"],  
4   "detail": {  
5     "state": ["stopping", "terminated"]  
6   }  
7 }
```

Copiar Patrón de prueba

Editar patrón

- o En la sección Objetivos a la derecha, configure los siguientes ajustes:



### Destino 1

**Tipos de destino**  
Seleccione un bus de eventos de EventBridge, un destino de la API de EventBridge (socio de SaaS) u otro servicio de AWS como destino.

☐ Bus de eventos de EventBridge  
☐ Destino de la API de EventBridge  
☒ Servicio de AWS

**Seleccione un destino** [Información](#)  
Seleccione los destinos que desee invocar cuando un evento coincida con el patrón de eventos o cuando se active la programación (hay un límite de 5 destinos por regla).

Tema de SNS ▼

Tema  
Default\_CloudWatch\_Alarms\_Topic ▼ ↺

► Configuración adicional

- En la parte inferior de la página, seleccione Configurar detalles.
- En la definición de regla, configure los siguientes ajustes:

### Detalles de la regla

**Nombre**  
Instance\_Stopped\_Terminated  
64 caracteres como máximo; se admiten números, letras en mayúscula o en minúscula y los caracteres „-“.

**Descripción - opcional**  
*Ingrese la descripción*

**Bus de eventos** [Información](#)  
Seleccione el bus de eventos al que se aplica esta regla, ya sea el predeterminado o uno de socios.  
default ▼

☒ **Habilitar la regla en el bus de eventos seleccionado**

**Tipo de regla** [Información](#)

☒ **Regla con un patrón de eventos**  
Regla que se ejecuta cuando un evento coincide con el patrón de eventos definido. EventBridge envía el evento al destino especificado.

☐ **Programar**  
Una regla que se ejecuta según una programación

Reglas (8) <span>↺</span> <span>Eliminar</span> <span>Habilitar</span> <span>Editar</span> <span>Plantilla de CloudFormation ▼</span> <span>Crear regla</span>						
<input type="text" value="Buscar reglas"/>			<span>Cualquier e...</span> <span>▼</span> <span>&lt; 1 &gt;</span> <span>⚙️</span>			
<input type="checkbox"/>	Nombre	Estado	Tipo	ARN	Descripción	
<input type="checkbox"/>	<a href="#">Instance_Stopped_Terminated</a>	<span>✔️</span> <b>Habilitado</b>	Estándar	arn:aws:events:us-west-2:107791249488:rule/Instance_Stopped_Terminated		

- Sobre los Servicios Menú, seleccione Servicio de notificación simple.
- En el panel de navegación izquierdo, seleccione Temas.
- Seleccione el enlace en la columna Nombre.



**Suscripciones (1)**

Editar Eliminar Solicitar la confirmación Confirmar la suscripción **Crear una suscripción**

Buscar

ID	Punto de enlace	Estado	Protocolo
bf46c2fd-e2c4-4386-be1...	josephh2408@gmail.com	Confirmada	EMAIL

- o Sobre los Servicios. En el menú, seleccione EC2.
- o En el panel de navegación izquierdo, seleccione Instancias.
- o Seleccione la casilla de verificación junto a Servidor web.
- o Elija el estado de la instancia, luego Detener instancia, y luego Detener.

**Instancias (1/1)** Información

Última actualización Hace 28 minutos Conectar Estado de la instancia Acciones Lanzar instancias

Buscar Instancia por atributo o etiqueta

	Name	ID de la instancia	Tipo de inst...	Comprobación de	Estado de la al	Zona d
<input checked="" type="checkbox"/>	Web Server	i-08caa9fe6947...	t3.micro	3/3 comprobador	Ver alarmas +	us-west

Detener instancia

Iniciar instancia

Reiniciar instancia

Hibernar instancia

Terminar (eliminar) instancia

- o Luego deberías recibir un correo electrónico con detalles sobre la instancia que se detuvo. El mensaje tiene formato JSON. Para recibir un mensaje más fácil de leer, puede crear una función AWS Lambda que CloudWatch Events active. La función Lambda podría formatear un mensaje más legible y enviarlo a través de Amazon SNS.

**AWS Notification Message** Recibidos x

**AWS Notifications** <no-reply@sns.amazonaws.com> para mí

Traducir al español

{ "version": "0", "id": "bad287da-afc5-d09a-c00e-b6027b7ef29b", "detail-type": "EC2 Instance State-change Notification", "source": "aws.ec2", "account": "107791249488", "time": "2024-10-04T22:58:25Z", "region": "us-west-2", "resources": [ "arn:aws:ec2:us-west-2:107791249488:instance/i-08caa9fe6947fdc6" ], "detail": { "instance-id": "i-08caa9fe6947fdc6", "state": "stopping" } }

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:  
[https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:107791249488:Default\\_CloudWatch\\_Alarms\\_Topic:bf46c2fd-e2c4-4386-be1a-9266393cf664&Endpoint=josephh2408@gmail.com](https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:107791249488:Default_CloudWatch_Alarms_Topic:bf46c2fd-e2c4-4386-be1a-9266393cf664&Endpoint=josephh2408@gmail.com)

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>



## TAREA 5

En esta tarea, activará las reglas de AWS Config para garantizar el cumplimiento del etiquetado y los volúmenes de Amazon Elastic Block Store (Amazon EBS).

- Sobre los Servicios Menú, seleccione Config.
- Si aparece un botón Comenzar, haga lo siguiente:
- En el panel de navegación izquierdo, seleccione Reglas (el que está hacia la parte superior).
- Seleccione Agregar regla
- En la sección Reglas administradas de AWS, en el campo de búsqueda, ingreserequired-tags
- Seleccione el botón junto a etiquetas obligatorias.

Reglas administradas por AWS (421)				
<div><input type="text" value="required-tags"/> 1 coincidencia</div>				
	Nombre ▲	Marcas	Modo de evaluación admitido	Descripción
	required-tags	AWS	DETECTIVE	Checks whether your resources have the tags that you specify.

- Elija Siguiente
- En la página Configurar regla, desplácese hasta Parámetros y configure los siguientes ajustes:



### Parámetros

Los parámetros de regla definen atributos que los recursos deben cumplir para cumplir con la regla. Los atributos de ejemplo incluyen una etiqueta obligatoria o un bucket de S3 especificado. Los parámetros **opcionales** que no son válidos, como la falta de una clave o un valor, no se guardarán.

Clave

tag1Key

Valor

project

- Seleccione Agregar regla
- En la sección Reglas administradas de AWS, en el campo de búsqueda, ingrese ec2-volume-inuse-check
- Seleccione el botón junto a ec2-volume-inuse-check.

Reglas administradas por AWS (421)			
ec2-volume-inuse-check		1 coincidencia	
Nombre	Marcas	Modo de evaluación admitido	Descripción
ec2-volume-inuse-check	EC2	DETECTIVE	Checks whether EBS volumes are attached to EC2 instances.

- Elija Siguiente
- Seleccione Siguiente nuevamente.
- Seleccione Agregar regla
- Espere hasta que se haya completado la evaluación de al menos una de las reglas. Actualice la página de su navegador si es necesario.
- Seleccione cada una de las reglas para ver el resultado de las auditorías.
- Bajo > Entre los recursos dentro del alcance, seleccione Conforme de la lista.

Recursos dentro del ámbito					Ver detalles	Solucionar	
Conforme					< 1 >		
ID	Tipo	Estado	Anotación	Conformidad			
<input type="radio"/> i-08caa9fe6947ffdc6	EC2 Instance	-	-	Conforme			

Recursos dentro del ámbito					Ver detalles	Solucionar	
Conforme					< 1 >		
ID	Tipo	Estado	Anotación	Conformidad			
<input type="radio"/> vol-06fe2ff28e5017f55	EC2 Volume	-	-	Conforme			